Distributed Security Controls in Industrial Control Systems

Adam Spanier
School of Interdisciplinary Informatics
University of Nebraska at Omaha
Omaha, NE USA
aspanier@unomaha.edu

Kendra Herrmann
School of Interdisciplinary Informatics
University of Nebraska at Omaha
Omaha, NE USA
kherrmann@unomaha.edu

Perry Donahue
School of Interdisciplinary Informatics
University of Nebraska at Omaha
Omaha, NE USA
pdonahue@unomaha.edu

Matthew Popelka
School of Interdisciplinary Informatics
University of Nebraska at Omaha
Omaha, NE USA
mpopelka@unomaha.edu

Brevin Wagner
School of Interdisciplinary Informatics
University of Nebraska at Omaha
Omaha, NE USA
bwagner@unomaha.edu

***Abstract*—Abstract here**

I. Introduction

Securing critical infrastructure assets based on distributed industrial control systems (ICS) is a difficult problem to solve [1] [2] [3]. This difficulty arises from two competing natures in critical systems: they *must* efficiently use computationally limited devices *and* they must be secure against attack and failure [3] [4] . On the one hand, a critical system must be fast, accurate, efficient, and robust; a list of requirements that, when associated with the innate computational imitations present in critical systems devices, presents notable difficulty in simply building a system that works. On the other hand, if the system is attacked or fails in some way, property may be damaged, people may die, and society may suffer; thus, the system *must be secure* [3] [4]. However, most security controls exhibit computationally intense algorithms that, if run on limited computing devices, can cause the system to slow down or, at the worst, crash. In this way, these systems *require* security but the very act of adding security controls to these systems becomes a *very real threat* to the security of the system itself.

These competing requirements present ICS designers and engineers with a dilemma: they must create a system that is fast, efficient, and functional using computationally limited equipment, while simultaneously implementing robust security controls that protect the system without degrading the speed and efficiency of the network [4]. In the midst of such a dilemma, the most common recourse generally reduces to the mutually exclusive implementation of either function *or* security. In a situation where designers are faced with such an ultimatum, functionality will always supersede security. A system that implements robust security measures yet lacks any real function is useless. The very reason the system is being designed is to solve a functional problem, not a security problem.

Though such a mutually exclusive solution allows the system to fulfill functional requirements, it leaves many modern critical systems open to a number of common security attacks [3] [4] [5]. For example, given a system where remote access must be achieved as quickly as possible, the implementation of laborious or time-consuming login protocols can be the difference between the loss of thousands of dollars, the damage to expensive equipment, or even the loss of life. In such an instance, designers will intentionally choose to avoid authentication mechanisms that are commonly used to prevent intrusions [3] [4]. In a system powered by computationally limited devices like PLCs or RTUs, computationally expensive encryption mechanisms can cause significant slow-downs and even denial-of-service outages. Again, with such limited computation and with a need for real-time cyber-physical responses, engineers will choose to forgo expensive security mechanisms so that their system can still meet the rigid and unmoving requirements set by the real-world environment the system serves.

As it stands, traditional security controls and methodologies simply do not meet the stringent computational requirements enacted by such limited systems [2]. In fact, many critical systems simply choose to avoid or accept the risk of cyber-security attacks through avenues that can easily be secured with encryption, authentication, and access controls. This reality necessitates a comprehensive and robust search for alternative security mechanisms; mechanisms that work symbiotically with the distributed nature of distributed ICS networks.

The study of cryptography is not new; nor is the investigation into novel types of cryptographic structures. A cryptographic structure is nothing more than the combination of cryptographic primitives into a new data- and functionally-oriented mechanism. One such cryptographic structure commonly used today is the blockchain. A blockchain is nothing more than a distributed record of data that uses data hashes, the digital signatures of the various entities operating within the blockchain environment, and the linked list data structure [6]. The distributed nature of the blockchain makes it compatible with most any type of distributed network. Due to it's distributed nature, it is the cornerstone cryptographic structure used by Bitcoin, the very first digital cryptocurrency successfully implemented [7]. The distribution-friendly nature of blockchains makes such a cryptographic structure interesting in the context of distributed ICS networks. Other cryptographic structures and methods like fingerprinting and distributed authentication present the same potential benefits if applied to distributed ICS networks.

This work aims to investigate alternative security mechanisms for distributed industrial control systems, specifically those based on distributed cryptographic architectures. The work will investigate how, if at all, these alternative security mechanisms can be integrated into distributed ICS networks, and what value, if any, these mechanisms add to the security profile of such a critical system.

To carry out this work, the following research questions are used:

1) How can Distributed Industrial Control Systems be designed for security using distributed cryptographic security controls?
2) How can these techniques be applied to and combined in ICS networks with limited computational capabilities as a means to increase security?

By answering the questions above, this work can begin to understand what, if any, benefits can be gained by applying distribution-friendly security mechanism to distributed instructional control systems. Given any benefit is discovered, even if marginal, such an improvement has the potential to provide real-world benefits to critical infrastructure systems by augmenting the security profile of the system. This improvement in security profile, even if marginal, when applied to worldwide critical systems architectures, presents a noticeable benefit to the stability of the systems that keep society running.

The rest of this work will be organized as follows: Section II details the background and foundational information needed to understand industrial control systems and operational technologies. Section III will explore existing works. Section IV will provide an emulation system design methodology, purpose, requirements, architecture, and design. Section V will outline the software used to emulate the system and explore the test system configuration. Section VI will analyze the testing regime for the emulated system. Section VII will discuss the outcomes and how the research questions were answered. Finally, section VIII will conclude the paper with a summation of the findings.

II. Background

A. Industrial Control Systems

An Industrial Control System (ICS) is a cyber-physical system that uses programs to control industrial processes, generally through sensing and actuating [8]. These systems use a device called a Programmable Logic Controller (PLC) to carry out the cyber-physical interactions in the industrial environment [9].

Most ICS networks operate within a distributed network. These networks connect distributed devices like PLCs to a centralized control hub. These centralized control hubs, called Supervisory Control and Data Acquisition (SCADA) systems, use a series of Remote Terminal Units (RTUs) to interact with the devices in the distributed network [10]. These SCADA systems encompass both the hardware and software assets implemented to carry out the SCADA system operations.

Most distributed ICS networks using SCADA system architectures operate in hard-real-time environments. Real-time environments are broken into two types: 1) soft-real-time and 2) hard-real-time. In hard-real-time environments, the tasks to which the system is responsible must be completed in a specific period of time [11]. In these systems, the operation *cannot* be late. If, at any point, the response of the system to some physical stimuli extends beyond the specified reaction time, the system fails.

SCADA systems in hard-real-time environments are not arbitrarily limited by the constraints of engineers or developers. Instead, they serve the whims of the physical domains to which they are tethered. For example, in the instance of a power substation, if voltage or currency exceeds proper limits, the system must act quickly to break the flow else collateral damage can be incurred.

Operational Technologies (OT) comprise any system in which the operational constraints outweigh the information requirements. Generally, OT is used interchangeably as a means to refer to ICS networks [12].

B. Decentralized Security Controls

A blockchain is a linked list that uses hash address as pointers to the next node [13]. A hash is nothing more than a low-cost, one-way algorithm that converts any number of input bits to a fixed number of output bits [13]. Blockchains are built as a means to provide immutability in time-scale transaction histories [13]. This is accomplished by hashing data, signing it, and adding this has as a reference from the previous block. In this way, the blockchain can record data in a time-linear fashion that cannot be changed after being added.

A digital signature is a unique value that is associated with one document and one key [13]. Much like a real-world signature would be associated with a real-world document, so also digital signatures associate one key to a single digital document. Digital signatures are accomplished by hashing the contents of a document, encrypting those contents with the private key of a public/private key pair, and affixing the encrypted hash to the document. If the hash can be decrypted using the public key and the hash that is decrypted using the key matches that of the document, the document can be proven unchanged and the signature associated with the private key. Digital signatures create non-repudiation, that is; digital signatures remove a user's ability to deny interactions with data [13].

Code Signing is much like digital signatures. The hash of a codebase is taken and signed by the company producing the code using their private key. This signature is then affixed to the executable or code artifact being published. The associated public key for the company's private key is made public alongside the executable code. To verify that the code hasn't been tampered with, a user must simply decrypt the signature using the public key, hash the executable downloaded, and compare the resulting hash to the result of the decrypted signature. If the two hashes are the same, the code has not been tampered with [13].

Digital fingerprinting is the process by which either data or physical attributes of a device are used to generate unique identifiers for different hardware and software applications [14]. Fingerprints can be used to identify devices via differences in hardware attributes. By observing heat, humidity, conductivity, weight, and other physical attributes of a device, an identifier unique to each device can be generated such that the device and only the device can produce the ID. This ID can be used to identify the PLC in logging and authentication processes. Fingerprints can also be used to identify common patterns in device functionality. If a PLC emits a steadily fluctuating set of RF signals, this fluctuation can be mapped and analyzed such that any variation from that fingerprint is indicative of an error in the system [14].

III. Related Work

A. Literature Review Methodology

This research uses a three step literature review methodology to generate a literature corpus for further analysis. The three steps used are: 1) the literature search, 2) literature selection, and 3) literature synthesis. The literature search sees a keyword-based search string applied to two research databases. The literature selection process applies specific criteria to each pertinent paper for inclusion into the research corpus. Finally, the literature synthesis section discusses the findings of the literature search.

The literature review sees a set of keywords combined into logical search strings. These strings are applied to two specific databases. The query results are analyzed and literature in the results that meets selection criteria are added to the research corpus. Upon the completion of the corpus, all added literature is analyzed, grouped, categorized, and discussed regarding relevance to the topic of this research.

1) Literature Search Keywords: The literature search uses the following keywords:

- PLC
- Programmable Logic Controller
- Blockchain
- Fingerprinting

These keywords are used due to their relevance to the topic at hand. Terms one (1) and two (2) relate to PLCs and terms three (3) and four (4) relate to decentralized or novel cryptographic applications.

The following terms are also used due to the discovery of emergent terminology in applying the search method:

- IIoT
- Industry 4.0

Based on the keywords above, the following search strings are used:

- PLC Blockchain
- PLC Fingerprinting
- Programmable Logic Controller Blockchain
- Programmable Logic Controller Fingerprinting
- IIoT
- Industry 4.0

2) Literature Search Databases: The following Databases will be used in this literature search:

- IEEE Xplore
- The ACM Digital Library

During the search, snowballing will be used to add pertinent literature to the selection candidates.

3) Literature Selection: To be added to the research corpus, each relevant literature candidate must be:

- relevant to the research topic
- published in either an IEEE or ACM sanctioned publication
- a full research paper
- written in English
- published within the last five (5) years

Upon addition to the research corpus, snowballing can be used to add related works to the literature corpus for review.

4) Literature Synthesis: Upon completion of the research corpus, the included literature will be analyzed for common themes. Literature with similar themes will be grouped together. Each grouping will be categorized and given a name. Each category will be described briefly based on the literature included, and an overview of the findings will be discussed.

B. Literature Review

After conducting the systematic literature review described above, nineteen (19) relevant pieces of literature were added to the research corpus. From these works, the following three (3) categories emerged: 1) Data Integrity Protection (DIP), 2) Device Fingerprinting (DF), and 3) Decentralized System Design (DSD). In the DIP category , two (2) sub-categories were identified: 1) Centralized Protection and 2) Decentralized Protection. In the DF category, two sub-categories were identified: 1) Anomalous Behavior Detection and 2) General Fingerprinting. In the DSD category, the following two (2) categories emerged: 1) Supporting Decentralized System Weaknesses and 2) Combining Decentralized Protections.

Of the nineteen (19) works analyzed in this literature review, ten (10) fell into the DIP classification. Of the 10 in the DIP classification, three (3) were added to the Centralized Protection classification and seven (7) to the Decentralized Protection classification. Six (6) of the works in this review were added to the DF classification. Of the six (6) works in the DF category, three (3) were added to the Anomalous Behavior

Detection sub category and three (3) were added to the General Fingerprinting sub-category. The remaining three (3) works were added to the DSD category. Of the three (3) in the DSD category, one (1) was added to the Supporting Decentralized System Weaknesses sub-category and two (2) were added to the Combining Decentralized Protections sub-category.

1) Data Integrity Protection: Relating to Centralized Data Protection, Colelli et al. [15] propose a blockchain ledger associated with an ICS Historian as a means to provide immutable data tracking for all PLC-related data via a data integrity scanner on the blockchain. Davis et al. [16] propose a blockchain-based traceability solution wherein all parts and processes of a given manufacturing system are logged, hashed, and appended to the blockchain for quality assurance validation. Schorradt et al. [17] chose to carry out a design much like Davis et al. but rather than a novel-private blockchain, the researchers chose to add the data to the public Ethereum blockchain. While the application created by Schorradt et al. worked, the use of the public Ethereum blockchain indicated prohibitively slow speeds for real-time operating systems.

Relating to Decentralized Data Protection, Choi et al. [18] propose a decentralized blockchain-based data storage system for both data protection and for secure, immutable logging in a Nuclear Power Plant. Otte et al. [19] propose a blockchain for process level traceability in mixing battery chemicals as a means to verify compliance with quality requirements and chemical regulations. Parvizimosaed et al. [20] present a decentralized ledger storage scheme that allows PLC data to be stored at the edge with the PLCs as a means to resist ransomware attacks. Garrocho et al. [21] present a novel blockchain based access control mechanism for cloud-based Industrial Internet of Things (IIoT) devices housed at the edge for faster and more secure PLC authentications. Jadidi et al. [22] carry out a blockchain much like other works in this category, but add a deep learning layer to help identify anomalous ICS behaviors. Kirkman et al. [23] provide a ransomware-resistant design that relies on OS-file locks and the ever-running nature of blockchain software to both resist and detect ransomware intrusions. Hayes et al. [24] created a ground-up Raspberri Pi-based communication ledger for IIoT-based decentralized data storage.

2) Fingerprinting: Relating to Anomalous Behavior Detection, Cook et al. [25] present a PLC fingerprinting mechanism using the memory contents of each PLC as a means to map memory patterns against known Memory Mapping conditions. Formby et al. [26] present a physics and timing-based fingerprinting mechanism wherein residual signals and timing artifacts are measured for each PLC as a means to accurately detect anomalous behavior. Lu et al [27] present a novel noise reduction scheme for the identification of time-based anomalies in IIoT traffic.

Relating to General Fingerprinting, Roy et al. [28] present an external, power consumption-based fingerprinting algorithm wherein the power signatures of PLCs are measured and documented in nominal operations and subsequently measured for anomalous behaviors. Keliris et al. [29] present a system wherein the application of modbus functionality allows the system to predict different PLC models. Kumar et al. [14] make a deep dive on the state of the art regarding all fingerprinting techniques and methodologies.

3) Decentralized System Design: Relating to the support of known decentralized system weaknesses, Garracho et al. [30] propose a failure model to help security professionals shore up known weaknesses in IIoT systems enabled with decentralized security.

Relating to the combination of decentralized protections in industrial control systems, Kannelonning et al. [1] categorizes security protections in Norwegian industry and Hosen et al. [31] design a prototype decentralized security system for an industrial control system.

C. Literature Review Discussion

Based on the literature review carried out in this research, the study of blockchain and decentralized functionality in industrial control systems is not new. Of the nineteen works covered in this review, ten of them fall in the blockchain or decentralized ledger classification. While the approach fell in two categories; that of centralized and decentralized, the consistent thread among all works lay in the novel application of some blockchain-type application in some industrial system, generally for the purpose of either distributed storage or for secure logging.

Further, the idea of using fingerprinting as a means to both identify devices and anomalies is also not a novel idea. While only six of the works cited in this study analyze fingerprinting, the state of the art well-known and well-explored. The most common use of fingerprinting in industrial control systems lies in the use of either power consumption, physics-based, timing-based, or memory-based analysis as a means to observe anomalous PLC or ICS behaviors. Other uses of fingerprinting lay in it's ability to uniquely identify any device.

Where this review found lacking information lay more in the observations of existing decentralized ICS research. Only three works fell in the Decentralized System Design classification. Of these three, each pushed at the problem from a different angle. Garracho et al. [30] simply tried to understand existing weaknesses and Kannelonning et al. [1] canvassed the Norwegian industry landscape for security controls. Hosen et al. [31] presented a novel combination of a number of decentralized ICS protocols to create a holistic design for a possible ICS network.

IV. System Design

A. System Design Methodology

How did we choose to design the system? Why did we choose to design the system in this way? Are there alternatives? What is our design plan? - Control ICS System for Baselines - Standard Protection ICS System - Decentralized Security Control Combinations

B. System Purpose

What does the system do? What devices are in the system? How does it function?

C. System Requirements

Assets in ICS Systems Threat/Asset Groupings Decentralized Security Controls and Threat Groups System Functional Requirements System Non-Functional Requirements

D. System Architecture

System Purpose? - What does this system do? System Components System Security Controls System Diagrams Functional Explanation of the system How does this design fit the methodology and does it solve the problem?

V. System Emulation

System Emulation Software Explanation Why did we choose this approach System Emulation Implementation Methodology How does the emulation system work? System Architecture System demonstration

VI. Testing

What tests will be use? How did we come up with these tests? How were the tests deployed? What are the raw results?

VII. Discussion

How did we attempt to answer the research questions? Did we actually answer them? If so, what is the answer?

VIII. Conclusion

Overview of the findings of the paper

References

[1] K. Kannelønning and S. Katsikas, "Deployment of cybersecurity controls in the norwegian industry 4.0," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, ser. ARES '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3664476.3670896

[2] J. C. Knight, "Safety critical systems: challenges and directions," in *Proceedings of the 24th International Conference on Software Engineering*, ser. ICSE '02. New York, NY, USA: Association for Computing Machinery, 2002, p. 547–550. [Online]. Available: https://doi.org/10.1145/581339.581406

[3] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, 2012.

[4] L. E. G. Martins and T. Gorschek, "Requirements engineering for safety-critical systems: Overview and challenges," *IEEE Software*, vol. 34, no. 4, pp. 49–57, 2017.

[5] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[6] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[7] M. Memon, S. S. Hussain, U. A. Bajwa, and A. Ikhlas, "Blockchain beyond bitcoin: Blockchain technology challenges and real-world applications," in *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 2018, pp. 29–34.

[8] C. M. Poskitt, Y. Chen, J. Sun, and Y. Jiang, "Finding causally different tests for an industrial control system," in *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, 2023, pp. 2578–2590.

[9] W. Alsabbagh and P. Langendörfer, "Security of programmable logic controllers and related systems: Today and tomorrow," *IEEE Open Journal of the Industrial Electronics Society*, vol. 4, pp. 659–693, 2023.

[10] M. M. Ahmed and W. L. Soo, "Customized scada system for low voltage distribution automation system," in *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific*, 2009, pp. 1–4.

[11] D. Leinbaugh, "Guaranteed response times in a hard-real-time environment," *IEEE Transactions on Software Engineering*, vol. SE-6, no. 1, pp. 85–91, 1980.

[12] M. Shilenge and A. Telukdarie, "Optimization of operational and information technology integration towards industry 4.0," in *2022 IEEE 31st International Symposium on Industrial Electronics (ISIE)*, 2022, pp. 1076–1081.

[13] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016. [Online]. Available: https://books.google.de/books?id=LchFDAAAQBAJ

[14] V. Kumar and K. Paul, "Device fingerprinting for cyber-physical systems: A survey," vol. 55, no. 14s, Jul. 2023. [Online]. Available: https://doi.org/10.1145/3584944

[15] R. Colelli, C. Foglietta, R. Fusacchia, S. Panzieri, and F. Pascucci, "Blockchain application in simulated environment for cyber-physical systems security," in *2021 IEEE 19th International Conference on Industrial Informatics (INDIN)*, 2021, pp. 1–7.

[16] W. Davis, M. Yaqoob, L. Bennett, S. Mihai, D. V. Hung, R. Trestian, M. Karamanoglu, B. Barn, and H. Nguyen, "An innovative blockchain-based traceability framework for industry 4.0 cyber-physical factory," in *Proceedings of the 2023 5th Asia Pacific Information Technology Conference*, ser. APIT '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 118–122. [Online]. Available: https://doi.org/10.1145/3588155.3588174

[17] S. Schorradt, E. Bajramovic, and F. Freiling, "On the feasibility of secure logging for industrial control systems using blockchain," in *Proceedings of the Third Central European Cybersecurity Conference*, ser. CECC 2019. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3360664.3360668

[18] M. K. Choi, C. Y. Yeun, and P. H. Seong, "A novel monitoring system for the data integrity of reactor protection system using blockchain technology," *IEEE Access*, vol. 8, pp. 118 732–118 740, 2020.

[19] S. Otte, L. Reuscher, D. Keller, and J. Fleischer, "Blockchain architecture for process-level traceability of continuous mixing process in battery cell production," in *2024 1st International Conference on Production Technologies and Systems for E-Mobility (EPTS)*, 2024, pp. 1–14.

[20] A. Parvizimosaed, H. Azad, D. Amyot, and J. Mylopoulos, "Protection against ransomware in industrial control systems through decentralization using blockchain," in *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, 2023, pp. 1–5.

[21] C. T. B. Garrocho, K. N. Oliveira, D. J. Sena, C. F. M. da Cunha Cavalcanti, and R. A. R. Oliveira, "Bace: Blockchain-based access control at the edge for industrial control devices of industry 4.0," in *2021 XI Brazilian Symposium on Computing Systems Engineering (SBESC)*, 2021, pp. 1–8.

[22] Z. Jadidi, A. Dorri, R. Jurdak, and C. Fidge, "Securing manufacturing using blockchain," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1920–1925.

[23] S. S. Kirkman, S. Fulton, J. Hemmes, C. Garcia, and J. C. Wilson, "A blockchain architecture to increase the resilience of industrial control systems from the effects of a ransomware attack: A proposal and initial results," *ACM Trans. Cyber-Phys. Syst.*, vol. 8, no. 1, Jan. 2024. [Online]. Available: https://doi.org/10.1145/3637553

[24] J. Hayes, A. Aneiba, and M. Gaber, "Symbiot: Towards an extensible blockchain integration testbed for iiot," in *Proceedings of the 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum*, ser. IIoT-NETs '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 8–14. [Online]. Available: https://doi.org/10.1145/3609389.3610565

[25] M. M. Cook, A. K. Marnerides, and D. Pezaros, "Plcprint: Fingerprinting memory attacks in programmable logic controllers," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3376–3387, 2023.

[26] Q. Gu, D. Formby, S. Ji, H. Cam, and R. Beyah, "Fingerprinting for cyber-physical system security: Device physics matters too," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 49–59, 2018.

[27] Z. Lu, "A robust anomaly detection approach for iiot time series," in *Proceedings of the 2024 2nd International Conference on Frontiers of Intelligent Manufacturing and Automation*, ser. CFIMA '24. New

York, NY, USA: Association for Computing Machinery, 2025, p. 168–173. [Online]. Available: https://doi.org/10.1145/3704558.3707091

[28] T. Roy and A. A. L. Beex, “Power measurement based code classification for programmable logic circuits,” in *2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2018, pp. 644–648.

[29] A. Keliris and M. Maniatakos, “Remote field device fingerprinting using device-specific modbus information,” in *2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2016, pp. 1–4.

[30] C. T. B. Garrocho, K. N. Oliveira, A. L. d. Santos, C. F. M. da Cunha Cavalcanti, and R. A. R. Oliveira, “Toward a failures model for communication of decentralized applications with blockchain networks applied in the industrial environment,” *IEEE Wireless Communications*, vol. 29, no. 3, pp. 40–46, 2022.

[31] A. S. M. S. Hosen, P. K. Sharma, D. Puthal, I.-H. Ra, and G. H. Cho, “Secblock-iiot: A secure blockchain-enabled edge computing framework for industrial internet of things,” in *Proceedings of the Third International Symposium on Advanced Security on Software and Systems*, ser. ASSS ’23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3591365.3592945